

**DATA PROCESSOR HAVING DATA PROCESSING UNIT
INCORPORATING SCRAMBLE AND DESCRAMBLE MEANS**

BACKGROUND OF THE INVENTION

1. Field of the Invention:

The present invention relates to a data processor having a means for scrambling data to be written to a data memory and a means for descrambling the scrambled data.

2. Description of the Related Art:

Currently, a data processor such as a so-called one chip microcomputer includes a data memory such as a RAM (Random Access Memory) and a data processing unit such as a CPU (Central Processing Unit) which are interconnected through a data bus and an address bus.

In such a data processor, since the data memory is connected with the data processing unit through the data bus, unauthorized acquisition of data transferred through the data bus is possible by probing from the outside.

Japanese Patent Laid-open Publication No.11-167526 and Japanese Patent Laid-open Publication No.11-203237 disclose data processors intended for preventing data from being leaked out as mentioned above. The data processors disclosed in these official gazettes are hereinafter described in brief.

First, the data processor disclosed in Japanese Patent Laid-open Publication No.11-167526 comprises, as shown in Fig. 1, RAM 101 serving as a data memory and CPU 102 serving as a data processing unit interconnected through address bus 103 and data buses 104, and further comprises scramble/descramble circuit 105 disposed at the midpoint of data buses 104.

Scramble/descramble circuit 105 scrambles data to be written to RAM 101 from CPU 102 and descrambles the scrambled data read from RAM 101 to CPU 102. Thus, in the data processor, probing of the stored states of memory cells in RAM 101 allows only the scrambled data to be acquired, and probing of data buses 104 between scramble/descramble circuit 105 and RAM 101 allows only the scrambled data to be acquired.

The data processor disclosed in Japanese Patent Laid-open Publication No.11-203237 comprises, as shown in Fig. 2, RAM 201 serving as a data memory and CPU 202 serving as a data processing unit interconnected through address bus 203 and data buses 204, and further comprises scramble/descramble circuits 205 and 206 incorporated in RAM 201 and CPU 202, respectively.

Thus, in this data processor, data to be written to RAM 201 from CPU 202 is transferred to RAM 201 through data bus 204 after being scrambled at scramble/descramble circuit 206 of CPU 202, and is written to RAM 201 after

being descrambled at scramble/descramble circuit 205.

Data to be read from RAM 201 to CPU 202 has also been scrambled by the time of transfer through data bus 204. Thus, in this data processor, probing of data bus 204 allows only the scrambled data to be acquired.

However, in the data processor shown in Fig. 1, probing of data bus 104 between scramble/descramble circuit 105 and CPU 102 permits unauthorized acquisition of data. In the data processor shown in Fig. 2, probing of the stored states in memory cells 207 of RAM 201 permits unauthorized acquisition of data.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a data processor capable of favorably preventing data leakage with a simple structure.

According to one aspect of the present invention, a data processor incorporates a means for scrambling data to be written to a data memory and a means for descrambling the scrambled data written in the data memory only in a data processing unit.

Since probing of the stored state of a data bus or memory cells in the data memory allows only the scrambled data to be acquired, it is difficult to obtain the original data before scrambling.

According to an embodiment of the present invention,

the scramble means scrambles data in accordance with a write address, and the descramble means descrambles the scrambled data in accordance with a read address.

Since the scrambled data is changed corresponding to the write address, it is difficult to obtain the original data by analyzing the scrambled data. In this case, all the bits of the data need not be scrambled, and some of the bits of the address may be used. Scrambling or descrambling of the data in accordance with the values of lower bits of the address makes it more difficult to obtain the original data by analyzing the scrambled data since the values of the lower bits are frequently changed.

According to another embodiment of the present invention, each of the scramble means and the descramble means comprises inverter means for inverting each of a plurality of bits at predetermined positions in data, and selector means for selecting each of the plurality of bits at the predetermined positions in the data or each of inverted bits obtained by inverting the bits in accordance with a value of a corresponding one of a plurality of bits at predetermined positions in a writing/reading address of the data.

According to another embodiment of the present invention, the data memory is divided into a plurality of areas based on addresses, and data is scrambled/descrambled in accordance with each area.

The above and other objects, features and advantages of the present invention will become apparent from the following description with reference to the accompanying drawings which illustrate examples of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram schematically showing main portions of a first prior art of a data processor;

Fig. 2 is a block diagram schematically showing main portions of a second prior art of the data processor;

Fig. 3 is a block diagram showing main portions of a data processor according to a first embodiment of the present invention;

Fig. 4 is a diagram showing divided areas of a RAM serving as a data memory in a data processor according to a second embodiment of the present invention; and

Fig. 5 is a block diagram showing main portions of the data processor of the second embodiment.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to Fig. 3, there is shown a data processor according to a first embodiment of the present invention, for example formed as a one chip microcomputer, and comprising RAM 301 serving as a data memory, CPU 302

serving as a data processing unit, data bus 303 and address bus 304 for connecting RAM 301 with CPU 302. Assume that data to be written to and read from RAM 301 includes four bits.

RAM 301 includes a number of memory cells 301' disposed in a matrix for storing data at individually specified addresses. CPU 302 executes various types of data processing, stores various data at determined addresses in RAM 301, and reads data from RAM 301. CPU 302 includes scramble circuit 305 and descramble circuit 306.

Scramble circuit 305 is connected to data bus 303 for scrambling data to be written to RAM 301 from CPU 302. Descramble circuit 306 is also connected to data bus 303 for descrambling the scrambled data read from RAM 301 by CPU 302.

Scramble circuit 305 comprises inverters 307₀, 307₁, 307₂ and 307₃ and selectors 308₀, 308₁, 308₂ and 308₃. Inverters 307₀, 307₁, 307₂ and 307₃ invert 0 bit D₀, 1 bit D₁, 2 bit D₂ and 3 bit D₃ in data, respectively. Selectors 308₀, 308₁, 308₂ and 308₃ output bits D₀, D₁, D₂ and D₃ respectively as they are when 0 bit A₀, 1 bit A₁, 2 bit A₂ and 3 bit A₃ of its address are "0", or when they are "1," output bits $\bar{D}_0$, $\bar{D}_1$, $\bar{D}_2$ and $\bar{D}_3$ obtained by inverting bits D₀, D₁, D₂ and D₃ by inverters 307₀, 307₁, 307₂ and 307₃, respectively. Descramble circuit 306 also

comprises inverters 309₀, 309₁, 309₂ and 309₃ and selectors 310₀, 310₁, 310₂ and 310₃. Inverters 309₀, 309₁, 309₂ and 309₃ correspond to inverters 307₀, 307₁, 307₂ and 307₃, while selectors 310₀, 310₁, 310₂ and 310₃ correspond to selectors 308₀, 308₁, 308₂ and 308₃, respectively.

If data to be written to RAM 301 by CPU 302 is, for example, "1110" with four lower bits of its address "0101", the data is scrambled into "1011" and written to RAM 301 through data bus 303. The data "1011" written to RAM 301 is input to CPU 302 through data bus 303 and descrambled into the original data "1110" by descramble circuit 306.

Therefore, probing of data bus 303 allows only the scrambled data to be acquired, and probing of the stored states of the memory cells in RAM 301 allows only the scrambled data to be acquired, thereby presenting favorable security for data.

In addition, in the embodiment, data is scrambled in accordance with its address and is not scrambled uniformly, thus making it difficult to obtain the original data by analyzing the scrambled data. Furthermore, since the address is used as the key for scrambling and descrambling, the scrambled data can be descrambled readily and reliably even when data is written in timing different from data reading.

Also, since lower bits of address data used as the key for scrambling and descrambling are changed frequently, the scrambling state of data also is frequently changed, thus making it more difficult to obtain the original data by analyzing the data.

Scramble circuit 305 and descramble circuit 306 comprise the plurality of inverters and selectors to enable the scramble and descramble circuits to be realized with a simple structure.

While the aforementioned embodiment illustrates scrambling and descrambling of all bits of data in accordance with lower bits of its address, the present invention is not limited thereto.

For example, it is possible to perform scrambling and descrambling by using predetermined bits other than the lower bits of an address as the key, or to scramble only some of the bits at predetermined positions in data. Since lower bits of an address are frequently changed as described hereinabove, the scrambling state can be frequently changed when they are used as the key. However, if it turns out that the lower bits of the address are the key for scrambling, the original data can be readily detected. In this case, arbitrary bits of the address are preferably used as the key for scrambling.

While the aforementioned embodiment illustrates a RAM as a data memory, any data memory may be used which

stores data corresponding to its address, and for example, a flash memory, an FD (Floppy Disc), or an MO (Magnetic Optical Disc) may be used.

Next, a second embodiment of the present invention will be described.

In a data processor of the second embodiment, as shown in Fig. 4, RAM 301 has four areas divided corresponding to addresses.

Additionally in the embodiment, as shown in Fig. 5, instead of direct input of address bits A_0 , A_1 , A_2 and A_3 to selectors 308₀, 308₁, 308₂ and 308₃ of scramble circuit 305, selector control circuit 401 is connected to selectors 308₀, 308₁, 308₂ and 308₃, and area determining circuit 402 is connected to selector control circuit 401.

Area determining circuit 402 receives all bits A_{11} , A_{10} , ..., A_0 of an address, determines its area (Area 1, Area 2, Area 3 or Area 4), and outputs to selector control circuit 401 an area signal of four bits with only a predetermined one bit being "1" as the determination result. Selector control circuit 401 comprises AND gates and OR gates, and outputs a selector control signal of four bits in a pattern corresponding to each area signal.

For descramble circuit 306, selector control circuit 401 and area determining circuit 402 are similarly provided. The address input to area determining circuit 402 may be some of the bits as long

as they enable the identification of the area.

In the embodiment, similar to the first embodiment, data is scrambled in accordance with address data and the scrambled data is descrambled in accordance with the address data, thereby making it more difficult to analyze the data.

While preferred embodiments of the present invention have been described using specific terms, such description is for illustrative purposes only, and it is to be understood that changes and variations may be made without departing from the spirit or scope of the following claims.

What is claimed is:

1. A data processor comprising:

a data memory;

a data bus for transferring data to be written to said data memory or read from said data memory;

an address bus for transferring an address for writing to said data memory or reading from said data memory; and

a data processing unit connected to said data memory through said data bus and through said address bus, for writing data at a specified address in said data memory and for reading data at a specified address in said data memory;

said data processing unit incorporating means for scrambling data to be written to said data memory and means for descrambling scrambled data read from said data memory.

2. The data processor according to claim 1, wherein said scramble means scrambles data in accordance with a write address, and said descramble means descrambles scrambled data in accordance with a read address.

3. The data processor according to claim 2,



wherein said scramble means inverts each of a plurality of bits at predetermined positions in data when a corresponding one of a plurality of bits at predetermined positions in a writing address is at a predetermined value, and said descramble means inverts each of a plurality of bits at said predetermined positions in scrambled data when a corresponding one of a plurality of bits at said predetermined positions in a reading address is at said predetermined value.

4. The data processor according to claim 3, wherein said plurality of bits in said address are lower bits.

5. The data processor according to claim 3, wherein each of said scramble means and said descramble means comprises:

inverter means for inverting each of a plurality of bits at predetermined positions in data; and

selector means for selecting each of said plurality of bits at said predetermined positions in said data or each of inverted bits obtained by inverting said bits in accordance with a value of a corresponding one of a plurality of bits at predetermined positions in a writing/reading address of said data.



6. The data processor according to claim 1, wherein said scramble means scrambles data in accordance with areas in said data memory divided previously on the basis of an address, and said descramble means descrambles scrambled data in accordance with said areas in said data memory.

7. The data processor according to claim 1, wherein each of said scramble means and said descramble means comprises:

inverter means for inverting each of a plurality of bits at predetermined positions in data;

selector means for selecting each of said plurality of bits at said predetermined positions in said data or each of inverted bits obtained by inverting said bits in accordance with a control signal;

area determining means for receiving all or some of bits of a write/read address of said data and for determining one of said plurality of areas in said data memory including said address; and

selector control means for outputting control signals at predetermined values to said selectors in accordance with said area determined by said area determining means.

